(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 September 2005 (09.09.2005)

PCT

(10) International Publication Number
WO 2005/083644 A1

(51) International Patent Classification[7]: G07F 7/08, G06F 17/60

(21) International Application Number: PCT/NL2004/000156

(22) International Filing Date: 2 March 2004 (02.03.2004)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **STIKKER.COM BV** [NL/NL]; De Lairessestraat 153, NL-1075 HK Amsterdam (NL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **MAYERS, Jeroen** [NL/NL]; Banstraat 10, NL-1071 JZ Amsterdam (NL). **KLEINHERENBRINK, Bernardus, Johannes, Paulus** [NL/NL]; Michelangelostraat 13, NL-1077 BN Amsterdam (NL).

(74) Agent: **VAN LOOIJENGOED, Ferry, Antoin, Theodorus**; De Vries & Metman, Overschiestraat 180, NL-1062 XK Amsterdam (NL).

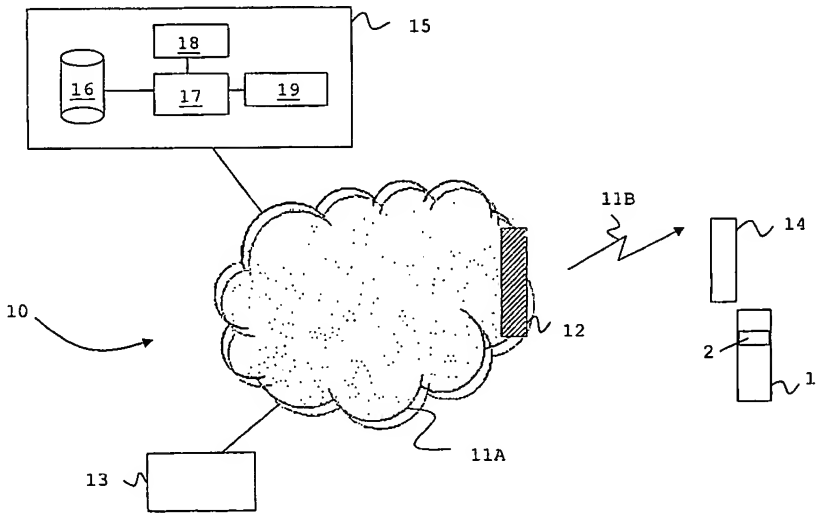
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: METHOD AND SYSTEM FOR VERIFYING THE AUTHENTICITY OF GOODS



(57) Abstract: The invention relates to a method and system for verifying the authenticity of one or more goods (1), each good (1) having at least one associated user-exposable code (2). The system comprises at least one authentication server (15) arranged to have access to unique codes for authentic goods and to verify said user-exposable code (2). A user device (13,14) is connected to said authentication server (15) via a data transmission network (11). A user of a user device (13,14) may transmit the user-exposable code (2) and an exposure state of said user-exposable code (2) to said authentication server (15). The authentication server (15) is arranged to determine the authenticity of said good (1) in dependence on said user-exposable code (2) and said exposure state. By considering the exposure state of the user-exposable code (2), counterfeit goods are more reliably identified.

WO 2005/083644 A1

Method and system for verifying the authenticity of goods

The invention relates to a method and system for verifying the authenticity of goods.

In recent years, a considerable need has been recognized for anti-counterfeiting methods and systems for use on a variety of articles or goods. Many of these methods and systems rely on special product features. However, an approach wherein the complexity of features goods is increased will only work for a limited period of time, as the large profits from counterfeiting gives counterfeiters access to advanced resources. Moreover, complex features are not always appreciated by customers and may require advanced education or knowledge of these customers. Further, such an approach raises manufacturing costs. Authenticity of products is particularly relevant for valuable items, items with a reputation of quality or products for which the quality is critical. Examples of such goods comprise jewellery, proprietary products, pharmaceutical products or spare parts for e.g. cars. Further such methods and systems may be useful for products with a weak distribution control.

WO 99/04364 discloses a method and system for verifying the authenticity of goods by marking these goods with random numbers and providing users with access to a database with codes of authentic goods. Comparing means are provided to compare the random number of a good with the codes in the database in order to verify the authenticity of the goods. If the database indicates that the code has previously been used, it is indicated to the user that the code is a duplicate, being evidence of illegal counterfeiting.

A disadvantage of this method and system is, *inter alia*, that such an approach still allows counterfeiting. The numbers attached to the goods may e.g. be copied from the products and attached to counterfeited goods. If the copied number is verified at the database before the original number, the consumer of the original good is wrongly informed that his good is forged if he checks the authenticity afterwards. If

bar codes are used, the consumer needs a scanner or code reader to verify the authenticity of the goods.

It is an object of the invention to provide an improved method and system for verifying the authenticity of goods.

This object is achieved by providing a method for verifying the authenticity of one or more goods, each good having at least one associated user-exposable code, in a system comprising at least one authentication server at least arranged to have access to unique codes for authentic goods and to verify said user-exposable code, and at least one user device connectable to said authentication server via a data transmission network, comprising the steps of:

- receiving one or more data-strings comprising said user-exposable code and an exposure state of said user-exposable code at said authentication server;
- determining the authenticity of said good in dependence on said user-exposable code and said exposure state.

This object is further achieved by providing a system for verifying the authenticity of one or more goods, each having at least one associated user-exposable code, comprising at least one authentication server arranged to have access to unique codes for authentic goods and to verify said user-exposable code and at least one user device connectable to said authentication server via a data transmission network, said authentication server being arranged to determine the authenticity of said good in dependence on said user-exposable code and said exposure state.

By providing the goods with non-exposed codes that can be exposed by the user or consumer of the goods, chances of illegal copying of codes in stores or at other stages in the production and distribution process, are significantly reduced. Further by considering the exposure state of the code in the authenticity verification process, chances of abuse are further reduced. The user can establish the authenticity of the good prior to using it. The system is self-explanatory and therefore simple for the user.

In a particularly advantageous embodiment of the invention, the method comprises the steps of:

- if said user-exposable code does not match with said unique codes, transmitting at least a first non-authenticity message to said user device;
- or else, determining whether said user-exposable code has previously been received;
- and, if said user-exposable code has not previously been received, transmitting a first authenticity message to said user device;
- or else, providing a query on said user device relating to said exposure state;
- receiving in response to said query said one or more data-strings comprising said exposure state at said authentication server;
- transmitting a second non-authenticity message or a second authenticity message to said user device, depending on said exposure state.

Contrary to the prior art, the fact that a code was previously used does not necessarily result in a non-authenticity message. Instead a further query is presented to the user to establish the exposure state, e.g. evaluating whether the originally non-exposed code was exposed by the user himself. If the user did expose the code himself while the code has already been received and/or checked, there is a good chance counterfeiters have exposed original codes and covered these or copied codes again, indicating that a forged article is at stake. In this case a non-authenticity message reading e.g. "this product is probably fake" or "this code is suspect" is presented to the user. If the good of the user has attached an already exposed code, probably a genuine product is resold. Accordingly an authenticity message is presented to the user, reading e.g. "this product is probably genuine". It should be appreciated that the order of the steps is irrelevant as long as this effect is achieved.

The exposure state may also relate to other characteristics of the code, e.g. the environmental circumstances

wherein the code is readable. It may e.g. be so that after exposure of the code, the code becomes unreadable after a particular period of time and may only be made visible once more by heating the label. In such a case, the exposure state relates to how the code was made visible again.

It is noted that the method and system for verifying the authenticity of goods may be combined with other measures to distinguish counterfeited and authentic goods.

The invention further relates to a computer program product with computer executable code portions for performing the method and to an authentication server arranged to perform this method.

Some further embodiments of the invention are presented in the dependent claims and described in more detail below.

The invention will be further illustrated with reference to the attached drawings, which schematically show a preferred embodiment according to the invention. It will be understood that the invention is not in any way restricted to this specific and preferred embodiment.

In the drawings:

Figs. 1A and 1B respectively show a good with a non-exposed code and an exposed code;

Fig. 2 shows a system for verifying the authenticity of goods according to an embodiment of the invention, and

Fig. 3 shows a flow chart for a part of the method for verifying the authenticity of goods according to an embodiment of the invention.

Figs. 1A and 1B show a good, article, product or item 1, such as jewellery, a mobile phone, a theatre ticket or a pharmaceutical product. The good 1 has an associated user-exposable code 2, that is covered by a code cover 3 in Fig. 1A and exposed, i.e. the cover is removed, in Fig. 1B. The cover may e.g. be removed by peeling off the cover or by scratching it away. Preferably, the cover 3 cannot easily be reattached over the code 2. The code may be attached to the product in various ways, such as by means of labels, tags or stickers.

Alternatively the code 2 may be applied directly to the product, e.g. by printing or engraving, thereby reducing the chance that the good 1 and code 2 are separated.

It is noted that the good 1 may have multiple codes 2 that are e.g. applied on top of each other, such that only a single code cover 3 is required. In that case the codes 2 may e.g. be applied on stickers that can be removed by different users in a distribution chain in order to verify the authenticity of the good 1.

The label, tag, sticker or good itself further comprises an address 4 for verifying the authenticity over a data transmission network as will be described below. The label, tag, sticker or good itself may further comprise information on the manner in which one should proceed to verify the authenticity. The user should e.g. be prompted to remove the code cover 3.

Codes 2 or batches of such codes can be sold to parties having interests in reducing counterfeiting in one or more markets, such a manufacturers of distributors of pharmaceutical products.

Fig. 2 shows a system 10 for verifying the authenticity of one or more goods 1, wherein each good 1 has at least one user-exposable code 2, as was shown in Figs 1A and 1B.

The system 10 comprises a data transmission network 11 comprising a wired data transmission network 11A, such as e.g. the internet, and a wireless data transmission network 11B that is communicatively connected to the wired network 11A via a gateway 12. The system 10 comprises a first user device 13, e.g. a computer arrangement, and a second user device 14, e.g. a mobile phone. Further the system 10 comprises an authentication server 15 communicatively connected with network 11 and having access to a database 16, comparing means 17, a counter 18 and a query generator 19. The database 16 comprises unique codes identifying authentic goods 1. Measures are taken to avoid hacking of the database 16.

The operation of the system 10 displayed in Fig. 2 is described with reference to Fig. 3 illustrating an embodiment

of the method for verifying the authenticity of goods 1 according to the invention.

In 21 a data-string is received from the user device 14 over the data transmission network 11 at the authentication server 15. The data-string comprises the user-exposable code 2, e.g. 12345 67890 00141, of the good 1. The code preferably has over ten positions to enhance the scalability of the method and system and to minimize chances of guessing correct codes. This feature can be further enhanced by employing alphanumeric codes, which is a preferred embodiment of the invention.

As the code can be transmitted wirelessly, the user may check the authenticity of the good 1 at the purchase point. The code is entered on a web page with the address provided on or with the good 1 and is e.g. a URL. A URL is always unique and cannot therefore reasonably be duplicated thereby enhancing the safety of the system.

In 22, the authentication server 15 may provide a confirmation query at the user device 14 to check whether the code entered by the user is correct. If the code is incorrect, the user is requested to enter the correct code; else the user confirms that he entered the correct code and the method proceeds to 23. This confirmation procedure reduces the chance of incorrect assessment of the authenticity of the good 1.

In 23 the comparing means 17 of the authentication server 15 compares the received code 2 with the unique codes for authentic goods 1 in the database 16. If the received code 2 does not match a unique code of the database 16, a first non-authenticity message 24 is transmitted to the user device 14. Accordingly it is determined that the good 1 is not authentic. Subsequently further information can be gathered on the good 1 at 25, e.g. by transmitting further queries to the user device 14, to identify and flag a counterfeit at 26. This further information provides valuable intelligence of these illegal activity.

If the received code 2 matches with a unique code for an authentic good 1 of the database 16, in 27 it is determined

whether the code 2 was received previously. If the code 2 is received for the first time, a first authenticity message 28 is transmitted to the user device 14. Accordingly it is established that the good 1 to which the code 2 is associated is an authentic good. In 29 further information can be provided for the user.

If it is determined in 27 that the code 2 has been received previously, the query generator 19 may provide a query 30 relating to the exposure state of the user-exposable code 2. The query may e.g. read: "did you expose this code yourself?".

If the response to the query 30 is negative ("no") an authenticity message 31 is transmitted to the user device 14. The authenticity message 31 may e.g. read: "This product is probably genuine". In 32 alternative verification may be applied, wherein the user may be guided through the alternative verification route. As an example, the label or tag may comprise unique other features to which the user can be pointed and queried. The user may e.g. be asked to provide information on certain characteristics of a hologram provided on the label. Again further information can be provided to the user device 14 in 33.

If the response to the query 30 is positive ("yes"), a non-authenticity message 34 is transmitted to the user device 14. The non-authenticity message 34 may e.g. read: "This product is probably fake". In such a case the code 2 may e.g. have been copied or covered again. Subsequently further information can be gathered on the good 1 at 35, e.g. by transmitting further queries to the user device 14, to identify and flag a counterfeit at 36. This further information provides valuable intelligence of these illegal activity.

It should be appreciated that further steps may be added to the method or steps may be performed in a different sequence. An example of a further step is the provision of the counter 18 allowing not only the determination of whether the code 2 was previously received but also the determination of the actual number of times the code 2 was received. The method

may thus further involve the definition of a threshold for the number of times a code is received and performing an appropriate action is such a threshold is achieved or exceeded. If e.g. the code 2 of a good 1 is received more than three times at the authentication server 15, the alternative verification 32 may be more detailed. Another modification of the method involves the input at the user device 13, 14 and receipt of the user-exposable code 2 as well as the exposure state at the authentication server 15 in step 21, i.e. the query 30 is made independent of the fact whether the code 2 was received before. In this case only a single input, involving both the code 2 and the exposure state, is necessary at the user device 13, 14. Other modifications or combinations of steps can be envisaged as well. The system provides a source for valuable information on both legal and illegal activities. The system establishes a direct contact with the end-user of the good 1 which can be valuable for other commercial purposes, such as advertising or updates. Illegal goods can be traced.

CLAIMS

1. Method for verifying the authenticity of one or more goods (1), each good (1) having at least one associated user-exposable code (2), in a system (10) comprising at least one authentication server (15) at least arranged to have access to unique codes for authentic goods and to verify said user-exposable code (2), and at least one user device (13,14) connectable to said authentication server (15) via a data transmission network (11), comprising the steps of:

- receiving one or more data-strings comprising said user-exposable code (2) and an exposure state of said user-exposable code (2) at said authentication server (15);
- determining the authenticity of said good (1) in dependence on said user-exposable code (2) and said exposure state.

2. Method according to claim 1, comprising the steps of:

- if said user-exposable code (2) does not match with said unique codes, transmitting at least a first non-authenticity message (24) to said user device (13,14);
- or else, determining (27) whether said user-exposable code (2) has previously been received;
- and, if said user-exposable code has not previously been received, transmitting a first authenticity message (28) to said user device (13,14);
- or else, providing a query (30) on said user device (13,14) relating to said exposure state;
- receiving in response to said query (30) one or more of said data-strings comprising said exposure state at said authentication server;
- transmitting a second authenticity message (31) or a second non-authenticity message (34) to said user device (13,14), depending on said exposure state.

3. Method according to claim 1 or 2, wherein said query (30) evaluates whether said user-exposable code (2) was

exposed by the user of said good (1) and, if a positive response is received, transmitting said second non-authenticity message (34), or else, transmitting said second authenticity message (31).

4. Method according to one or more of the preceding claims, wherein said method further comprises the step of counting the number of times said user-exposable code (2) is received.

5. Method according to claim 4, wherein a threshold is defined for the number of times said user-exposable code (2) is received and, if said threshold is reached or exceeded, one or more alternative verification steps (32) are triggered.

6. Method according to one or more of the preceding claims, wherein said method further comprises the steps of:

- providing a confirmation query (22) on said user device (13,14) relating to the correctness of said received user-exposable code (2);
- checking (23) said user-exposable code (2) against said unique codes only after receiving a confirmation message from said user device (13,14) confirming the correctness of said user-exposable code (2).

7. Method according to one or more of the preceding claims, wherein said good (1) further comprises an access address of said authentication server (15), enabling a user to verify the authenticity of said good (1) over said data transmission network (11).

8. Method according to one or more of the preceding claims, wherein a plurality of codes (2) is associated with said good (1) and said authentication server (15) receives said codes (2) from a plurality of users in a distribution channel and compares said codes (2) with said unique codes.

9. Method according to one or more of the preceding claims, wherein said users expose said one or more user-exposable codes (2) by peeling off or scratching away a code cover (3).

10. Method according to one or more of the preceding claims, wherein said non-authenticity messages (24,34) and/or

said authenticity messages (28,31) are accompanied by or followed by further information for said user device (13,14) or a user of said user device (13,14).

11. Method according to one or more of the preceding claims, wherein one or more of said queries (22,30) and/or messages (24,28,31,34) are transmitted or received at least partly over a wireless data transmission network (11B).

12. Computer program product for verifying the authenticity of one or more goods (1), each good (1) having at least one associated user-exposable code (2), in a system (10) comprising at least one authentication server (15) at least arranged to have access to unique codes for authentic goods and to verify said user-exposable code (2), and at least one user device (13,14) connectable to said authentication server (15) via a data transmission network (11), at least including computer executable code portions for:

- receiving one or more data-strings comprising said user-exposable code (2) and an exposure state of said user-exposable code (2) at said authentication server (15);
- determining the authenticity of said good (1) in dependence on said user-exposable code (2) and said exposure state.

13. Computer program product according to claim 12, further comprising software code portions for performing the method of at least one of the claims 2-6, 8 and 10.

14. System (10) for verifying the authenticity of one or more goods (1), each good (1) having at least one associated user-exposable code (2), comprising at least one authentication server (15) arranged to have access to unique codes for authentic goods and to verify said user-exposable code (2) and at least one user device (13,14) connectable to said authentication server (15) via a data transmission network (11), said authentication server (15) being arranged to determine the authenticity of said good (1) in dependence on said user-exposable code (2) and said exposure state.

15. System according to claim 14, wherein said system (10) further comprises a query generator (19) for providing a

query (30) on said user device (13,14) relating to the exposure state of said user-exposable code (2).

16. Authentication server (15) for verifying the authenticity of one or more goods (1), each good (1) having at least one associated user-exposable code (2), said authentication server (15) being arranged to:

- receive one or more data-strings comprising said user-exposable code (2) and an exposure state of said user-exposable code (2), and
- determine the authenticity of said good (1) in dependence on said user-exposable code (2) and said exposure state.

17. Authentication server (15) according to claim 16, wherein said authentication server (15) further comprises a query generator (19) arranged to provide a query (30) to said user device (13,14) relating to said exposure state of said user-exposable code (2).

18. Authentication server (15) according to claim 16 or 17, wherein said authentication server (15) is further arranged to transmit authenticity messages (28,31) and non-authenticity messages (24,34) to said user device (13,14).

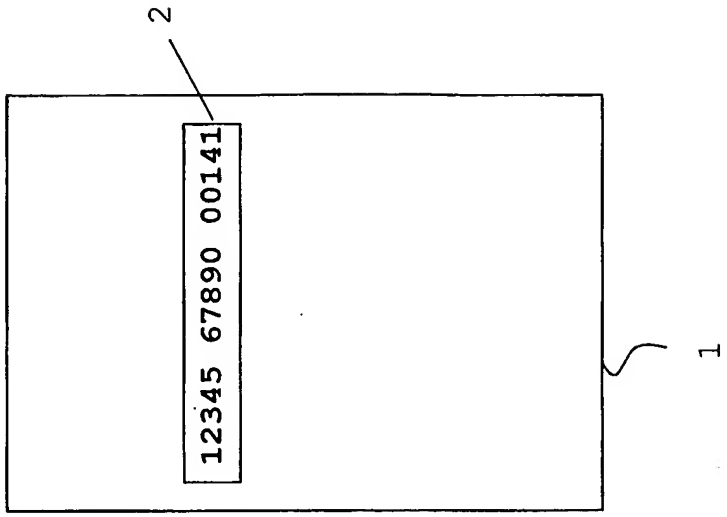


Fig. 1B

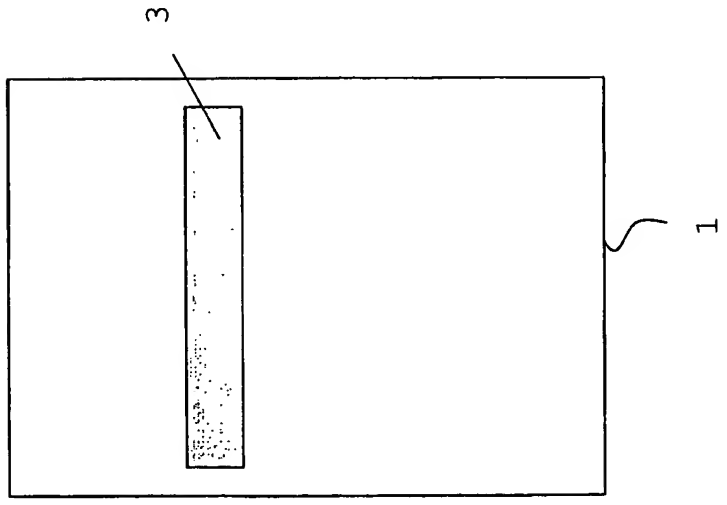


Fig. 1A

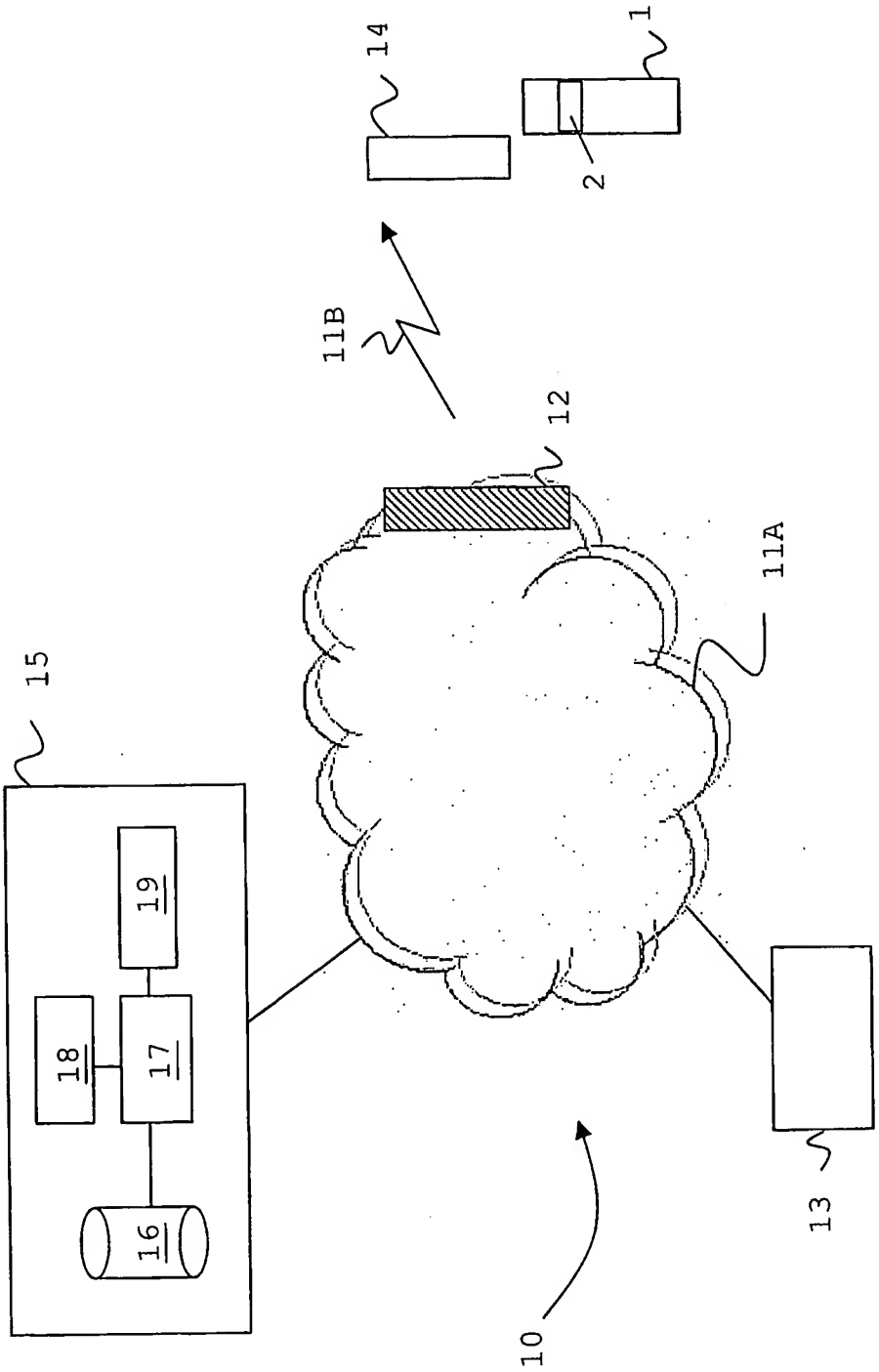


Fig. 2

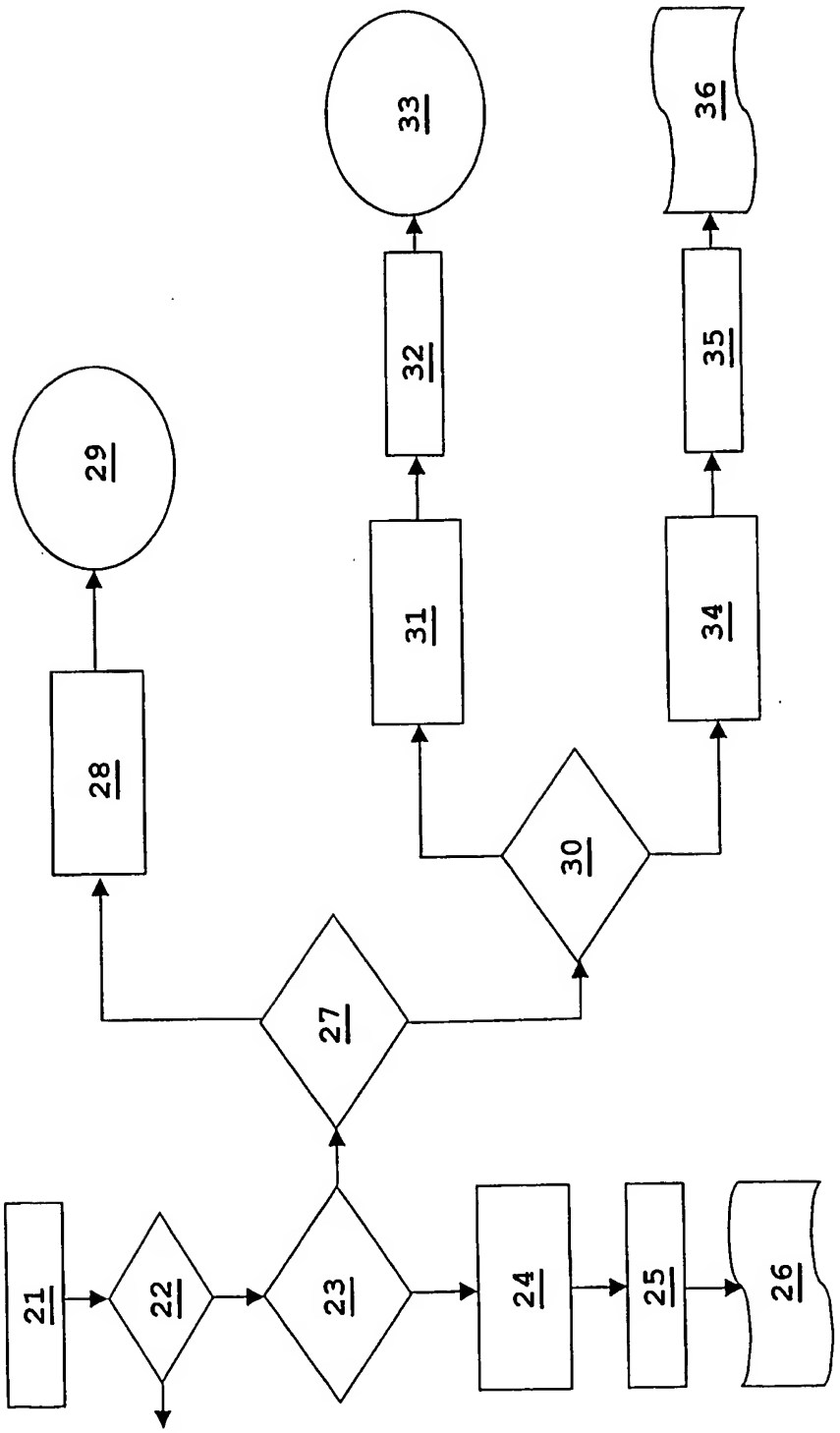


Fig. 3

INTERNATIONAL SEARCH REPORT

ıtional Application No
. . ./NL2004/000156

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/08 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the International search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 99/04364 A (ASSURE SYSTEMS, INC.) 28 January 1999 (1999-01-28) cited in the application page 3, line 15 - page 8, line 12 page 9, line 12 - page 14, line 12 page 22, line 15 - page 23, line 22 figures 1-3,6	1-18
X	WO 93/22745 A (CIAS, INC.) 11 November 1993 (1993-11-11) page 7, line 2 - page 14, line 32 page 15, line 16 - page 32, line 26; figures 1-3 claims 43,45	1-18

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 November 2004	09/12/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Neppel, C

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

	itional Application No
	/NL2004/000156

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 592 561 A (MOORE LEWIS J) 7 January 1997 (1997-01-07) column 3, line 22 - column 6, line 36 column 8, line 49 - line 63 column 22, line 8 - line 65	1-18
A	US 4 816 824 A (KATZ RONALD A ET AL) 28 March 1989 (1989-03-28) the whole document	1-18
A	EP 0 957 459 A (ORELL FUESSLI GRAPH BETR AG) 17 November 1999 (1999-11-17) the whole document	1-18
A	US 5 768 384 A (BERSON WILLIAM) 16 June 1998 (1998-06-16) column 2, line 24 - line 64	1-18

INTERNATIONAL SEARCH REPORT

ational Application No
/NL2004/000156

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9904364	A	28-01-1999	US	6442276 B1	27-08-2002
			AT	268486 T	15-06-2004
			AU	8577898 A	10-02-1999
			CA	2297683 A1	28-01-1999
			DE	69824291 D1	08-07-2004
			EP	0996928 A1	03-05-2000
			WO	9904364 A1	28-01-1999
WO 9322745	A	11-11-1993	WO	9322745 A1	11-11-1993
			AU	1895992 A	29-11-1993
			DE	69232519 D1	02-05-2002
			EP	0647342 A1	12-04-1995
US 5592561	A	07-01-1997	US	2003023557 A1	30-01-2003
			US	6456729 B1	24-09-2002
			US	6005960 A	21-12-1999
			US	5895073 A	20-04-1999
			US	5917925 A	29-06-1999
			US	6246778 B1	12-06-2001
US 4816824	A	28-03-1989	US	4423415 A	27-12-1983
			US	4558318 A	10-12-1985
			US	4651150 A	17-03-1987
			US	4739322 A	19-04-1988
			AT	16860 T	15-12-1985
			AT	67328 T	15-09-1991
			AU	7414281 A	19-01-1982
			BR	8108661 A	25-05-1982
			CA	1160749 A1	17-01-1984
			CA	1180814 A2	08-01-1985
			DE	3173107 D1	16-01-1986
			DE	3177255 D1	17-10-1991
			DK	75782 A	22-02-1982
			EP	0054071 A1	23-06-1982
			EP	0155982 A1	02-10-1985
			EP	0298156 A2	11-01-1989
			FI	820488 A	12-02-1982
			JP	6016312 B	02-03-1994
			JP	57500851 A	13-05-1982
			NO	820552 A	23-02-1982
			US	4785290 A	15-11-1988
			WO	8200062 A1	07-01-1982
			US	4489318 A	18-12-1984
			US	4546352 A	08-10-1985
			US	4568936 A	04-02-1986
			US	4663622 A	05-05-1987
			US	4675669 A	23-06-1987
			US	4476468 A	09-10-1984
			AT	90170 T	15-06-1993
			CA	1213371 A1	28-10-1986
			DE	3382689 D1	08-07-1993
			DE	3382689 T2	09-09-1993
			EP	0131574 A1	23-01-1985
			JP	7020781 A	24-01-1995
			JP	60500466 T	04-04-1985
			WO	8403019 A1	02-08-1984
EP 0957459	A	17-11-1999	EP	0957459 A1	17-11-1999

INTERNATIONAL SEARCH REPORT

ational Application No
/NL2004/000156

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5768384 A	16-06-1998	NONE	